AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH O.WUTTKE@SCHRNIDT-CLEMENS.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.	)	Case No. 19-MJ-119-JFJ

APPLICATION FOR A SEARCH WARRANT

I, SA Evan Held, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A":

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030	Computer Intrusion
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1956	Money Laundering
18 U.S.C. § 371	Conspiracy

The application is based on these facts:

See Affidavit of FBI SA Evan Held, attached hereto.

☑ Continued on the attached sheet.

☑ Delayed notice of ___ days (give exact ending date if more than 30: 8/6/2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Evan Held, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8-7-19

Judge's signature

City and state: Tulsa, OK Tulsa, Oklahoma

U.S. Magistrate Judge Jodi F. Jayne
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH O.WUTTKE@SCHRNIDT-CLEMENS.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

The Affiant, Evan D. Held, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Affiant makes this affidavit in support of an application for a search warrant for information associated with a certain account which is stored at premises controlled by Google LLC, an e-mail and cloud services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC ("Google") to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Affiant is a Special Agent of the Federal Bureau of Investigation (FBI), and has been so employed since graduation from the FBI's New Agent Training in Quantico, Virginia on February 15, 2013. Affiant is currently assigned to the Oklahoma City Division, Tulsa Resident Agency. As a Special Agent, Affiant's duties include, but are not limited to, investigating violations of federal criminal law and threats to national security. Affiant's investigations into

violations of federal law include, but are not limited to, computer intrusions, identity theft, threatening communications, and terrorism.

3. Affiant is familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, reviews of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open source information including information available on the Internet. Since this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact Affiant or others have learned during the course of this investigation.

4. Based on Affiant's training, experience, and the facts as set forth in this affidavit, Google account O.WUTTKE@SCHRNIDT-CLEMENS.COM contains evidence and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer intrusions), 1343 (wire fraud), 1956 (money laundering), and 371 (conspiracy),(collectively the "Subject Offenses").

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).]

6. When the Government obtains records pursuant to §2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the Government may obtain an

order precluding Google LLC from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b)

PROBABLE CAUSE REGARDING THE SUBJECT OFFENSES

7. Since May 2019, the FBI has been investigating the unauthorized intrusion into the corporate e-mail account of a Tulsa, Oklahoma-based oil and gas engineering firm (the "Victim Company"), in what appears to be a business e-mail compromise ("BEC") scam.

8. Based on Affiant's training, research and experience investigating cybercrime, Affiant knows, in part, the following about BEC scams:

a. A BEC scam typically involves the use of a fraudulent e-mail to direct a corporate employee to wire corporate funds to a bank account likely controlled by the perpetrators of the fraud (the "criminal perpetrators")

b. In one typical form of BEC fraud, the criminal perpetrators will gain access to a corporate computer network through a variety of techniques including, but not limited to, spear-phishing schemes designed to obtain a user's credentials. Using that access, criminal perpetrators will frequently study the corporate vendors, billing systems, and the style of e-mail communications for the corporation. Once the criminal perpetrators have familiarized themselves with the organization and the methods of communication, the criminal perpetrators will act. The criminal perpetrators can impersonate a legitimate employee or vendor in an attempt to cause the recipient to initiate a wire transfer to an account likely controlled by the criminal perpetrators.

9. The FBI was first contacted by a Vice President at the Victim Company (hereinafter referred to as "B.H.") on or about May 6, 2019. B.H. reported unknown individual(s) obtained unauthorized access to her e-mail account and modified payment wiring instructions on invoices.

10. The Victim Company's business activities involve buying equipment, repackaging, and selling it to end users. Invoices for purchases are typically sent via e-mail. The Victim Company conducts business with companies around the world to include Netherlands-based Schmidt + Clemens GmbH + Co. KG (Schmidt-Clemens).

11. B.H. previously communicated with Schmidt-Clemens employee Oliver Wuttke (Wuttke), and B.H. expected invoices to come from Wuttke. A review of e-mails provided by B.H. showed Wuttke's legitimate e-mail address was o.wuttke@schmidt-clemens.de.

12. On or about April 1, 2019, B.H. received an e-mail with a "revised" invoice from e-mail address o.wuttke@schrnidt-clemens.com (the "Subject Account"). Affiant noted the Subject Account substituted the letters "r" and "n" for the letter "m" in "schmidt[.]" Based on Affiant's training and experience, Affiant believes the unknown subject was attempting to masquerade as a legitimate vendor by using a slightly altered e-mail address which was very similar to Wuttke's legitimate e-mail address.

13. As a result of receiving an e-mail with a "revised invoice" from the Subject Account on or about April 1, 2019, B.H. contacted the Victim Company's bank via telephone and arranged for the wire transfer of approximately $686,199.00 USD. The wire was sent to an account at the Bank of China HK LTD.

14. On or about May 6, 2019, Wuttke contacted B.H. about the status the status of an outstanding payment which had not yet been received. In response, B.H. began reviewing her e-mails from Schmidt-Clemens in more detail and observed the difference between the legitimate

e-mail address and the Subject Account. Wuttke further advised B.H. the bank details were manipulated on the invoice from the Subject Account e-mail address, and the beneficiary bank account on the invoice did not belong to Schmidt-Clemens.

PROBABLE CAUSE REGARDING THE SUBJECT ACCOUNT(S)

15. On or about May 31, 2019, Affiant performed research on the domain "schrnidt-clemens.com" and identified the domain's mail exchange server as aspmx.l.google.com. Based on Affiant's training, research, and experience, this mail exchange server indicates Google is the e-mail service provider for the "schrnidt-clemens.com" domain.

16. On or about June 3, 2019, a 2703(d) Order was issued in the Northern District of Oklahoma to Google for records (not including content) pertaining to the Subject Account. After reviewing the non-content records provided by Google, Affiant located transactional records of e-mails between employees at the Victim Company and the Subject Account. The transactional records, in part, revealed the following information:

a. On or about February 26, 2019, the Subject Account sent an e-mail to B.H., among other recipients.

b. On or about February 26, 2019, the Subject Account received an e-mail from B.H., among other recipients.

c. On or about March 4, 2019, the Subject Account sent an e-mail to B.H., among other recipients.

d. On or about April 1, 2019, the Subject Account sent an e-mail to B.H., among other recipients.

17. Affiant reviewed the subscriber information provided by Google and noted the Subject Account was created on or about February 26, 2019, and accessed approximately seven

times between on or about February 26, 2019 and on or about April 1, 2019. Affiant learned approximately six of the seven IP addresses used to login to the Subject Account were assigned to an Internet Service Provider in Nigeria.

PROBABLE CAUSE REGARDING A COMPUTER INTRUSION

18. During interviews with employees at the Victim Company, Affiant learned B.H.'s Office 365 account had global administrator privileges.

19. Through online research, Affiant learned global administrators can access all administrative features in the Office 365 suite of services. Global administrators are the only administrators who can assign other admin roles, and only global administrators can manage the accounts of other global administrators.

20. During an interview on May 31, 2019, B.H. advised she never made any administrative changes in Office 365 to include adding, changing, or removing mailbox permissions or setting up e-mail rules on Victim Company's e-mail accounts.

21. The FBI received a copy of the Office 365 log file from the Victim Company. Upon reviewing the log file, Affiant identified log entries which appeared to correspond to B.H.'s Office 365 account modifying permissions or modifying e-mail rules on Victim Company's e-mail accounts, and identified approximately 16 unique IP addresses associated with the modifications. Affiant learned approximately 10 of the 16 unique IP addresses corresponding to the modifications were assigned to an Internet Service Provider in Nigeria.

BACKGROUND CONCERNING GOOGLE

22. In the Affiant's training, research, and experience, Affiant knows individuals involved in business e-mail compromise scams often use multiple e-mail accounts to compartmentalize and obfuscate their activity.

23. In the Affiant's training, experience, and research, Affiant knows e-mail providers such a Google usually maintain the following records and information with respect to subscriber accounts:

a. *E-mail content.* In general, any e-mail (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the e-mail providers' servers unless and until the subscriber deletes the e-mail. If the subscriber does not delete the e-mail, it can remain on the provider's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on the provider's servers for a certain period of time.

b. *Address Book.* E-mail providers usually also allow subscribers to maintain the equivalent of an address book, comprising e-mail addresses and other contact information of other e-mail users.

c. *Device Information.* E-mail providers can collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers, Mobile Electronic Identify Numbers, Mobile Equipment Identifiers, Mobile Identification Numbers, Subscriber Identity Modules, Mobile Subscriber Integrated Services Digital Network Number, International Mobile Subscriber Identifiers, or International Mobile Equipment Identities.

d. *Subscriber and billing information.* The e-mail provider can collect and maintain (typically unverified) identifying information about each subscriber, including, for

example, name, username, address, telephone number, and alternate e-mail addresses. The e-mail providers can also maintain records concerning the date on which the account was created, the Internet Protocol address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the e-mail provider can also maintain records of the subscriber's means and source of payment, including a credit card or bank account number

e. *Cookie Data.* E-mail providers can use features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at the e-mail provider using the same computer. One of the ways e-mail providers accomplish this is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by the e-mail provider when a computer visits its website or logs into an account.

f. *Transactional Information.* The e-mail providers typically retain certain transactional information about the use of an account. This information can include records of login (i.e. session) times and durations and the methods used to connect to the account.

g. *Location History.* E-mail providers can also collect data on the location of their users from their electronic devices. E-mail providers use this information for, among other things, location-based advertising, location-based search results, embedding location information in photographs and videos taken by the user (known as geo-tagging), navigation through maps and services and related

applications, and features that permit users to locate their mobile electronic devices if they lose them.

h. *Customer correspondence.* E-mail providers can also maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

i. *Preserved and backup records.* E-mail providers can also maintain preserved copies of the foregoing categories of records with respect to an account, for 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. Section 2703(f).

24. In the Affiant's training, experience, and research, Affiant has learned Google also maintains records with respect to other Google services, which it stores in connection with e-mail accounts, which can include, in part, the following:

a. *Google Drive Content.* Google can provide users with a certain amount of free cloud storage, which is currently approximately 15 gigabytes, through a service called Google Drive. Users can purchase a storage plan through Google to store additional content. Users can use their Google Drive to store e-mail, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google can provide users with the ability to write, edit, and collaborate on various documents with other Google users through a service

called Google Docs. Users can use Google Docs to create online documents which can be stored on or saved to the user's Google Drive.

c. *Google Photos.* Google can provide users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to store photographs and videos. Google also retains the metadata-or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata can include what is known as exchangeable image file format (EXIF) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appoints, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which can permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's e-mail and chat content.

f. *Location History Data.* Google can maintain recent location data, collected periodically, from mobile devices that are logged into or have used applications or

services provided by Google. For example. Google can collect information collected from GPS, or Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location Google applications and services can also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Chrome Browser and Search History.* Google can store information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

25. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In Affiant's training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail

communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described above, e-mail providers typically log the Internet Protocol addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

REVIEW OF INFORMATION OBTAINED PURSUANT TO THE WARRANT

26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to Google LLC, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the Government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence and instrumentalities of the Subject Offenses as specified in Attachment B to the proposed warrant.

27. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all information within the Subject Account(s). This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, Affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any keywords that an agent is likely searching for.

REQUEST FOR SEALING

28. Affiant respectfully requests this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions

from this matter. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation. As set forth above, the target(s) of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

CONCLUSION

29. Based on the forgoing, Affiant requests that the Court issue the proposed search warrant. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Evan D. Held
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 7th day of August, 2019

Honorable Jodi F. Jayne
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California and applies to all content and other information within the Provider's possession, custody, or control associated with the e-mail account O.WUTTKE@SCHRNIDT-CLEMENS.COM (the "Subject Account").

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on May 24, 2019, the Provider is required to disclose the following information to the government for each account listed in Attachment A:

1. *E-mail Content.* All e-mails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each e-mail, the data and time at which each e-mail was sent, and the size and length of each e-mail), limited to items sent, received, or created between February 26, 2019 and present;
2. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.
3. *Google services information.* The files and contents with the account related to Google services, including Google Drive, Google Docs, Google Photos, Google Calendar, Google Chats, Google Hangouts, Google Photos, Web and Search History, and Google Payments.
4. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username,

address, telephone number, alternate e-mail addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

5. *Search and web history records.* All records relating to web and application activity history (including search terms), device information history, and location history.

6. *Device information.* Any information identifying the device or devices used to access the Subject Account, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identify Numbers ("MEIN), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the Subject Account.

7. *Information Regarding Linked Accounts, Including Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Account, including specifically by cookie, Google Account ID, Android ID, or other account or device identifier (the "Linked Accounts").

    a. The following information regarding the customers or subscribers of the Linked Accounts:

1. Names (including subscriber names, user name, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol addresses and port numbers) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

8. *Location Data.* All location data associated with the Subject Account, including GPS data, cell site/cell towner triangulation/trilateration, and Wi-Fi location, including the GPS coordinates and dates and times of all location recordings.
9. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.
10. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

11. *Preserved or backed up records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. Section 2703(f) or otherwise.

Google is further ordered to disclose the above information to the Government within 14 days after service of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer intrusions), 1343 (wire fraud), 1956 (money laundering), and 371 (conspiracy),(collectively the "Subject Offenses"), including information pertaining to the following matters:

a. E-mail communications with the Victim Company;

b. Any information related to the Victim Company;

c. Information identifying the user or the location of the user of the Subject Account, and the individual involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Account, communications with individuals that the user of the Subject Account trusts, which reveal his/her identity to include information that can be used to ascertain his/her identity, such as travel information or receipts for online purchases or other communications with social network websites or third party service providers;

d. Communications of the user of the Subject Account with co-conspirators and others about the Subject Offenses, including but not limited to obtaining unauthorized access to the data from computer systems, reconnaissance of victim computer systems, victim selection and targeting, malicious software, software vulnerabilities, malicious domains, phishing e-mails, and monetizing stolen personal and computer system information belonging to other individuals, and communications and other data identifying such co-conspirators;

e. Communications and documents concerning the wiring or transferring of funds between bank accounts;

f. Phishing e-mails seeking to induce individuals to click on hyperlinks, download attachments, or otherwise take action to infect victim systems with malware, and test versions of the same;

g. Evidence concerning the user's technical expertise;

h. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

i. Information regarding the registration of other e-mail accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, and payment for such online facilities or services; and

j. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature